

REMARKS

Claims 1-8, 16, 19, 22, 24-25, and 28 are pending. Claims 1-8, 16, 19, 22, 24-25, and 28 stand rejected under 35 U.S.C. § 112, ¶ 2 as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. Claims 1-4, 7-8, and 16 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Merjanian. Claims 1 and 3 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patents No. 6,269,348, 5,870,723, and 5,838,812.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-8, 16, 19, 22, 24-25, and 28 remain in the case for consideration.

In rejecting claims 1-4, 7-8, and 16 under 35 U.S.C. § 102(e), the Examiner referred to the reference only as "Merjanian", and was not specific as to which patent by Merjanian was intended. Because the Examiner cited U.S. Patent No. 5,546,471 on form PTC-892, the Applicant is operating on the premise that this was the intended Merjanian patent.

Terminal disclaimers will be filed to overcome the double patenting rejection once the claims are otherwise allowable over the art of record.

REJECTION OF CLAIMS UNDER 35 U.S.C. § 112, ¶ 2

The Examiner has rejected claims 1-8, 16, 19, 22, 24-25, and 28 as being indefinite. The Examiner has indicated "the transmission of a structured data object or textual element" uses a "token" as defined in *Computer Dictionary*, 2nd Edition. (Incidentally, the Applicant notes that the Examiner did not include the copy of this reference, as indicated, nor was it cited on form PTO-892. The Applicant requests that the Examiner cite the reference in the next communication.) Because the transmission requires a token, the Examiner asserts that the term "tokenless" is indefinite.

The Examiner is misinterpreting the claims. The term "tokenless" does not refer to "tokens" in the sense of computer communication. Instead, "tokenless" refers to physical tokens such as smartcards and magnetic swipe cards, as recited in the last two lines of independent claims 1 and 3. For example, at page 13, lines 4-5, the specification recites that "[i]t is the essence of this invention that the Scrip Supporter not be identified through the direct use any man-made personalized tokens to effect a scrip transaction." The claims describe a system and method by which a scrip transaction can be implemented without using such a token.

It is clear that the Examiner understands this point: in the rejection under 35 U.S.C. § 102(e) over Merjanian, the Examiner states that Merjanian "do[es] not involve a smart card and thus, is "tokenless". It seems apparent that the Examiner is using the convenient fact that the term "token" has multiple meanings, and is ignoring context. If the Examiner understands the intended usage of the term "tokenless" as described, and as recited in the claims, the claim is on its face not indefinite.

In addition, the Examiner has indicated that claims 1 and 3 include a negative limitation, which he apparently considers indefinite. The Applicant does not traverse this rejection per se, as this phrase clarifies the term "tokenless". But the Applicant thinks that removing this phrase would render the claims less clear, especially in light of the Examiner's misunderstanding of the term "tokenless". And removing both the term "tokenless" and the phrase "without the scrip supporter presenting any smartcards or magnetic swipe cards" would change the claim from its intended meaning: the claims would less well-define the invention.

With reference to claims 5-6, 19, 22, 24-25, and 28, the Examiner has indicated that the claims are improperly presented Markush recitations. The Applicant disagrees. The claims are not Markush groups, but simply lists from which particular features can be selected. It is worth noting that there is generic language available: for example, in claim 22, the list shows different types of biometrics. Even if viewed as Markush groups, the Examiner does not identify any defect in their presentation. Accordingly, these claims are not improperly presented.

REJECTION OF CLAIMS UNDER 35 U.S.C. § 102(e)

Merjanian teaches an ergonomic fingerprint reader apparatus. The apparatus is designed in such a way as to support easy and comfortable reading of a fingerprint. Merjanian goes on to provide some example applications (columns 9-12), but the focus of Merjanian is on the device itself, not its uses.

In rejecting the claims, the Examiner has ignored the requirements of the MPEP. According to MPEP 706.02, "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present." The problem is that Merjanian omits several key elements of the claims.

First, nowhere does Merjanian mention the term "scrip". "Scrip" is a term that is used in the claims: for example, in the terms "electronic scrip transaction" and "scrip supporter".

But Merjanian does not use the term "scrip" or disclose or inherently include any equivalent thereof therefore, Merjanian cannot anticipate these features of the claims. Accordingly, claims 1-4, 7-8, and 16 are patentable under 35 U.S.C. § 102(e) over U.S. Patent No 5,546,471 to Merjanian, and are therefore allowable.

But even putting aside whether Merjanian teaches all of the features of the claims, the Examiner appears to misunderstand a basic difference between the claimed invention and Merjanian. Merjanian is directed toward an apparatus using biometrics to authorization and verification of individuals, whereas the patent application is directed toward methods using biometrics to identify individuals. To help illustrate the difference between the terms, the Examiner is invited to consider the plain meaning of the terms. "Identification" refers to the process of identifying someone: that is, "identification" answers the question of "Who am I?". Note that this question is open-ended, and the answer is the person's identity.

In contrast, "verification" and "authorization" refer to the process of confirming that a previously-provided identity is correct. In other words, these processes answer the question of "Am I who I say I am?". A common example of verification and/or authorization is the use of personal identification numbers (PINs) used at ATMs. It should be readily apparent that anyone could slide the ATM card into the machine. To help verify that the person using the card is the person authorized to use the card, the person has to enter the PIN that corresponds to the card. If the provided PIN matches that associated with the card then the user is presumed to be the proper user; if not, then the transactions are refused.

This difference is important, because verification and authorization and two-step processes; identification is a one-step process. In verification and authorization systems (such as Merjanian), the user must first somehow identify himself to the system. This is typically accomplished by providing something assigned uniquely to a single person (although not necessarily usable only by that person): for example, a credit card. A credit card has an account number that identifies a single person. This makes verification and authorization very easy: the biometric needs to be compared with only the biometric associated with that credit card number. If the provided biometric matches the biometric associated with the account, then the user is verified or authorized; if it does not match, then the user is not verified or authorized.

Although the above discussion centers on credit cards, a person skilled in the art will immediately recognize that any uniquely identifying information can be used to identify the individual. Most people have many different identifying data; they simply do not recognize it. For example, social security card numbers, bank account numbers, and numbers assigned

by other registrars (e.g., universities or doctor's offices) all uniquely identify people, to name but a few examples.

The Examiner might respond that certain numbers, such as a credit card account number, do not uniquely identify a person. For example, typically a husband and wife share the same credit card account number. The Applicant acknowledges this fact. But this does not change the fact that Merjanian teaches a verification or authorization system. Even if multiple people are associated with a particular identifying data, the system is still only attempting to verify or authorize the individual: the system still responds with either a "yes" or "no" message, depending on whether the provided biometric matches a biometric associated with the single account. This shows that Merjanian is not teaching a system to *identify* individuals: the system cannot say which user associated with the account provided the biometric; the system can only indicate that some user, whose biometric is associated with that one account, is accessing the account.

It should now be clear that prior art systems, like Merjanian, are two-step processes: they depend on the user to first identify himself or herself before he or she can be verified/authorized. Merjanian glosses over this fact, but this first step is implicitly discussed. For example, at column 10, lines 34-36, Merjanian says that "the person presenting the card or stamps is compared with a store of authorized operators". In other words, before the comparison can be made, the authorized operators must be identified. This theme is constant in Merjanian: each example requires the user to first identify himself or herself, before the comparison can be made.

The Examiner has referred to column 11, lines 1-21 of Merjanian, and asserted that they do not involve a smart card, and therefore are "tokenless". But this analysis ignores the fact that Merjanian does not teach identification of users. Thus, implicit in the discussion at the top of column 11 is the premise that, somehow, the user identifies himself first. For example, at column 11, lines 19, Merjanian states that "[d]uring identification, the individual's fingerprint data is again acquired, but this time is compared to the previously stored fingerprint data to determine whether the individual requesting benefits is entitled to receive the requested benefits". In other words, Merjanian compares the acquired fingerprint data to the data previously stored for the individual. This one-to-one comparison cannot be made unless the individual has been previously identified. This shows that Merjanian, as stated above, is doing verification, not identification.

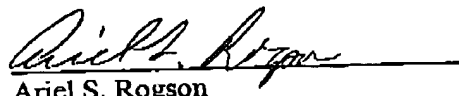
In addition, Merjanian does not enable biometric identification. Nowhere does Merjanian teach how biometric identification could be performed. The reason Merjanian

does not teach this is simple: Merjanian describes an apparatus to read fingerprints, and happens to expound on uses for such an apparatus. Describing the full implementation of such a use of the reader is beyond the scope of Merjanian, and indeed, is not his invention.

Finally, it is incorrect to say that there is no token involved. At column 11, lines 6-7, Merjanian describes storing the fingerprint data "on a card of the types previously described". Clearly, such a card is a token.

For the foregoing reasons, reconsideration and allowance of claims 1-8, 16, 19, 22, 24-25, and 28 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,
MARGER JOHNSON & McCOLLOM, P.C.


Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
Customer No. 20575